PATENT ABSTRACTS OF JAPAN

(11)Publication number : **2000-011075**
(43)Date of publication of application : **14.01.2000**

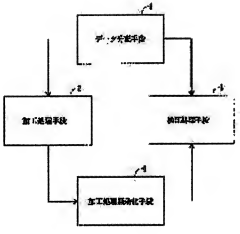
(51)Int.Cl. **G06F 19/00**
G06F 17/60
G09C 1/00

(21)Application number : **10-178413**
(22)Date of filing : **25.06.1998**

(71)Applicant : **FUJITSU LTD**
(72)Inventor : **SAOTOME MAKOTO**

(54) **DATA PROCESSOR**

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a means for shortening processing time by asynchronously executing settlement processing in parallel with data verification processing without waiting the verification processing in respect to a data processor for collectively working plural data with electronic (E) signs for preventing the generation of alteration.
SOLUTION: The data processor is provided with a data distribution means 1 for distributing data to be inputted while adding an identification(ID) code for allowing E sign verification processing data to correspond to the working processing data to the distributed data, a working processing means 2 for inputting the distributed working processing data and working the inputted data, a verification processing means 3 for inputting the verification processing data distributed in parallel with the processing of the means 1 and verifying the E sign, and a working processing invalidating means 4 for invalidating the working processing of the working processing data corresponding to the ID code when the E sign of the verification processing data is not verified.



LEGAL STATUS

[Date of request for examination]	29.07.2003
[Date of sending the examiner s decision of rejection]	16.08.2005
[Kind of final disposal of application other than the examiner s decision of rejection or application converted registration]	
[Date of final disposal for application]	
[Patent number]	
[Date of registration]	
[Number of appeal against examiner s decision of rejection]	2005-017694
[Date of requesting appeal against examiner s decision of rejection]	15.09.2005
[Date of extinction of right]	

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－11075
（P2000－11075A）
(43)公開日　平成12年１月14日(2000.1.14)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）
Ｇ０６Ｆ　19/00		Ｃ０６Ｆ　15/30	３６０	５Ｂ０４９
17/60		Ｃ０９Ｃ　1/00	６４０Ｂ	５Ｂ０５５
Ｇ０９Ｃ　1/00	６４０		６６０Ｂ	
	６６０	Ｃ０６Ｆ　15/21	３４０Ａ	
		15/30	Ｌ	

審査請求　未請求　請求項の数２　ＯＬ　（全６頁）

(21)出願番号　特願平10－178413

(22)出願日　平成10年６月25日(1998.6.25)

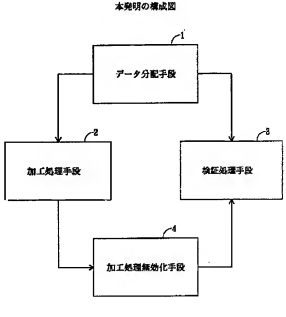
(71)出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号
(72)発明者　早乙女　真
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
(74)代理人　100072590
弁理士　井桁　貞一

Ｆターム（参考）　5B049 AA04 AA05 BB46 CC39 DD04 EE23 GG01 GG02
5B055 BB10 CB09 EE27 HB06 JJ00 KK05

(54)【発明の名称】　データ処理装置

(57)【要約】
【課題】　本発明は改ざんを防止する電子署名付複数のデータを一括して加工処理するデータ処理装置に関し、データの検証処理を待たず、決済処理を検証処理を並行して非同期に行い、処理時間の短縮を実現する手段を提供することを目的とする。
【解決手段】　入力するデータを電子署名の検証処理用データと加工処理用データを対応付ける識別符号を付加して分配するデータ分配手段１と、分配された加工処理用データを入力して加工処理する加工処理手段２と、上記加工処理手段と並行して分配された検証処理用データを入力して電子署名を検証する検証処理手段３と、検証処理データの電子署名の検証が得られない場合に識別符号が対応する加工処理データの加工処理を無効とする加工処理無効化手段４とを備えるように構成する。

本発明の構成図



【特許請求の範囲】
【請求項1】　改ざんを防止する電子署名付複数のデータを一括して加工処理するデータ処理装置であって、
入力するデータを電子署名の検証処理用データと加工処理用データを対応付ける識別符号を付加して分配するデータ分配手段と、
分配された加工処理用データを入力して加工処理する加工処理手段と、
上記加工処理手段と並行して分配された検証処理用データを入力して電子署名を検証する検証処理手段と、
検証処理データの電子署名の検証が得られない場合に識別符号が対応する加工処理データの加工処理を無効とする加工処理無効化手段と、をなすデータ処理装置。
【請求項2】　改ざんを防止する電子署名付複数のデータを一括して加工処理するプログラムであって、
コンピュータを、
入力するデータを電子署名の検証処理用データと加工処理用データに対応付ける識別符号を付加して分配するデータ分配手段、
分配された加工処理用データを入力して加工処理する加工処理手段、
上記加工処理手段と並行して分配された検証処理用データを入力して電子署名を検証する検証処理手段、
検証処理データの電子署名の検証が得られない場合に識別符号が対応する加工処理データの加工処理を無効とする加工処理無効化手段、として機能させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は改ざんを防止する電子署名付複数のデータを一括して加工処理するデータ処理装置に関する。
【０００２】
【従来の技術】例えば、電子マネーのように価値データ情報をネットワークあるいは電子媒体により受け渡すときにそこに示される情報が発生した時点から改ざんされていないことを確認して受け渡しの処理を完結しなければならない。個別の電子マネーによる商品購入、サービス授受のお金の支払いを金融機関が決済処理するときには、流通企業などにより商品購入に関する電子マネーデータが定期的に集められ、金融機関に受け渡され、一括して自動振替のような方法で買い物をした個人の口座から引き落とされる。
【０００３】従来のクレジットカードにおける自動引き落としと同様のデータの受け渡しであるが、情報がすなわちお金であり、電子マネーの使用者が商品購入時に対価として支払った内容、すなわち商品購入明細が正しく決済処理のデータとして受け渡されたことを保証するために途中でデータの改ざんがされていないかを検証するようになっている。すなわち電子署名の検証が行われて初めて正しいデータであることを認識して決済処理が行われる。
【０００４】電子署名は各商品購入データの明細、例えば、購入した事業者、店舗、日付、時刻、購入者の口座、購入金額などをハッシュ関数（ＭＤ４／５，ＳＨＡなど）のような一方向関数によりメッセージダイジェストが元のデータの特徴的なパターンとして抽出され元のデータに付加して受け渡すものである。受け取ったデータについて同じハッシュ関数によりメッセージダイジェストを作成して照合することで元のデータが改ざんされていないことを確認できる。
【０００５】従来の電子マネーの決済処理は図８の従来技術の説明図に示すように、一括して処理するデータについて上記改ざんが行われていないことを検証する処理が完了するのを待って商品購入者の口座からのお金の移動を行う決済処理を行っていた。図８に示すように電子署名の検証処理中にできる範囲でのチェック処理などは並行して行うことはできたが決済処理は検証処理の完了を待って行っていた。
【０００６】
【発明が解決しようとする課題】しかしながら、上記決済処理データは電子署名そのものの複雑化のほか、電子署名による確認のみではなく、データ、署名の暗号化、同封する暗号のキーの暗号化など何重にもデータセキュリティの強度を上げるための処理が施されるようになってきた。このため、入力データの検証処理に多くの時間が必要となってきた。このように検証処理に多くの時間がかかると、上記従来の処理方式では本来の決済処理の開始時間が遅れることにより日常の業務処理時間の延長などが問題でありその解決策が求められるようになった。
【０００７】本発明はこのような点にかんがみて、従来の流通系企業のように金融機関との取引の実績があり、電子マネーの使用された時点から一括して処理する商品購入データを金融機関に持ち込むまでの間にほとんど問題が発生しないようなデータについては、データの検証処理を待たず、決済処理を検証処理を並行して非同期に行い、総合的な処理時間の短縮を実現する手段を提供することを目的とする。
【０００８】
【課題を解決するための手段】上記の課題は下記の如くに構成された改ざんを防止する電子署名付複数のデータを一括して加工処理するデータ処理装置によって解決される。
【０００９】図１の本発明の構成図において、１は入力するデータを電子署名の検証処理用データと加工処理用データを対応付ける識別符号を付加して分配するデータ分配手段、２は分配された加工処理用データを入力して加工処理する加工処理手段、３は上記加工処理手段と並行して分配された検証処理用データを入力して電子署名

を検証する検証処理手段、4は検証処理データの電子署名の検証が得られない場合に識別符号が対応する加工処理データの加工処理を無効とする加工処理無効化手段を示す。

【００１０】電子署名付複数のデータはそれぞれの処理単位データ毎にそのデータの発生時に以後最終的に受け渡した先での加工処理までの情報伝達過程において内容に不法な変更（改ざん）が行われていないことを保証するための電子署名を付加されている。

【００１１】電子署名の検証処理と本来のデータの加工処理を非同期に並行処理するためにデータ分配手段１により、入力するデータを電子署名の検証処理用データと加工処理用データに分配する。後刻、分配したデータの対応付けを行うために各データに識別符号を付加して置く。

【００１２】検証処理手段３は本来加工のために受け渡されたデータを１件ずつ取り出し、データ発生元で電子署名を作成したものと同じハッシュ関数でメッセージダイジェストを作成し、付加されている電子署名と照合する。

【００１３】加工処理手段２は分配されたデータを順次取り出し、その内容の検証は待たず並行して本来のデータ加工処理を行う。検証処理手段３が検証できない電子署名を検出したときには、加工処理無効化手段４が起動され、識別符号が対応するデータの加工処理を無効化するようにしている。

【００１４】

【発明の実施の形態】図２には本発明の実施の形態の説明図を示す。実施の形態として、ＩＣカードを利用した電子マネーによる商品購入に付随する金融機関、電子マネーの運用を行う事業体（ＥＭ事業体と表示する）、商品販売する流通系企業相互間の電子マネー、価値情報の流れにかかわるデータ処理を示す。また、図３には本発明の実施の形態の構成図を示す。

【００１５】本実施の形態においては、パーソナルコンピューター、ワークステーション等の汎用的な目的で使用される計算機上で実行するコンピュータプログラムにより実現する形態を示す。

【００１６】本発明のデータ処理装置は、処理装置、主記憶装置、補助記憶装置、入出力装置などから構成される計算機上で、コンピュータプログラムを実行して実現される。また、コンピュータプログラムは、フロッピーディスクやＣＤ－ＲＯＭ等の可搬型媒体やネットワーク接続された他の計算機の主記憶装置や補助記憶装置等に格納されて提供される。本発明の記録媒体は、上記可搬型媒体、主記憶装置、補助記憶装置に該当する。

【００１７】提供されたコンピュータプログラムは、可搬型媒体から直接計算機の主記憶装置にロードされ、または、可搬型媒体から一旦補助記憶装置にコピーまたはインストール後に、主記憶装置にロードされて実行する。また、ネットワーク接続された他の装置に格納されて提供された場合も、他の装置からネットワークを経由して受信後に、補助記憶装置にコピー、主記憶装置にロードされ実行するものである。

【００１８】まず、図２により本発明の実施の形態の環境を説明する。電子マネーの仕組みは種々あるが、ここに示すものは、電子マネーの運用事業体（ＥＭ事業体）が金融機関の個人口座からＩＣカードに移動した個人の電子マネー資金を管理し、実際に商品購入に電子マネーが使用された情報に基づいて流通企業から請求されたとき、管理された個人の電子マネー資金と金融機関の個人口座と請求した流通企業の口座との間の自動振替決済を行う方式である。

【００１９】２１は金融機関で管理されている個人の口座である。ＩＣカードに電子マネーを移動するように端末を操作すると、２４でＥＭ事業体はＩＣカード２７に資金を移動するとともに、２５で個人別電子マネー資金情報を管理する。２８で商店、自動販売機などにより商品、サービスを購入すると対価としてＩＣカードにある電子マネーの価値情報がＰＯＳ端末などに移動し、合わせて購入された商品の明細が記録される。

【００２０】このとき商品購入による電子マネーの移動の内容が、最終的に金融機関、流通系企業の間で決済処理が行われるまで確実に受け渡されるように電子署名が作成され明細データに添付される。この電子署名は明細のデータをハッシュ関数で変換して作成されるもので、例えば１２８ビット（ＭＤ４／ＭＤ５）とか１６０ビット（ＳＨＡ）の長さの圧縮データである。

【００２１】流通系企業は２９で上記電子署名付で顧客の購入データ（明細）を回収する。また、２６では流通系企業はこれらのデータを請求データとして定期的にまとめてＥＭ事業体に受け渡す。このときも各請求の明細データには電子署名が付けられた状態で受け渡される。

【００２２】請求データを受け取ったＥＭ事業体は２３において請求データの明細を検証するとともに、２２において決済処理として自動振替を行う。すなわち、商品購入した個人口座管理２１、電子マネーの個人別資金情報管理２５と２０に示される企業の口座との間で振替処理を行い決済するのである。

【００２３】図３は本発明の実施の形態の構成図である。上記のように電子マネーが使われた結果、個人口座から企業口座へ最終的なお金の移動が決済処理されるところで本発明が適用される。図３にしたがって実施の形態を説明する。

【００２４】従来技術の説明で示したように決済処理を行うとき暗号強度を保証するためにデータのセキュリティを検証する時間が多く必要になっている。従来はデータの検証処理が完了するのを待って決済処理を行っていたところを、本発明では検証処理３４と並行して決済処理３３を実行するようにしている。

【００２５】決済処理３３は電子マネーを使用して商品を購入した個人の口座から商品を販売した企業の口座へ商品購入データに基づいて振替を行う。このとき、受け渡されたデータは改ざんが行われていないことを前提に処理することになる。商品購入データ３１は３２で分配されて決済に必要な情報は決済処理３３に渡される。複数の商品購入データは、これから決済処理されるもの、処理中のもの、決済処理済のものと３つの状態がある。

【００２６】複数の商品購入データの検証処理３４は決済処理３３が進行中に同じ順序で並行して実行されるが、検証処理の結果の確認されるタイミングは一般的には前後にずれる。しかしデータのセキュリティの強化に伴い検証処理の時間が多くかかることになり、各データの検証処理は多くは決済後になる。

【００２７】流通系企業の回収する商品購入データの信頼度が高く減多におこり得ないことではあるが、万一電子マネーの利用時点から決済処理が行われる時点までになんらかのデータの改ざんが行われていたときには検証処理３４の実行中にエラーとして検出される。このエラーをきっかけとして並行して処理が進んでいる決済処理３３に通知する。

【００２８】決済処理３３はエラーの通知を受けたときには未処理の商品購入データあるいは処理中のデータに対する処理の停止を行う。既に決済処理済のデータについては取消処理３５を実行する。

【００２９】フローチャートで動作を説明する前に、電子署名の生成と確認について説明する。図４に商品購入データの形式の説明図を示す。４２はＩＣカード上の電子マネーを使って商品の購入をしたときに明細データとして記録されるものである。この商品購入の明細データ４２はネットワーク、電子媒体により伝達され決済処理されるまで変更されることなく受け渡されなければならないものである。

【００３０】明細データ４２が作成された時点であらかじめ定められたハッシュ関数によりメッセージダイジェストを作成して電子署名Φ４３として明細データ４２に添付する。なお、４１は流通系企業が複数の明細データをまとめてＥＭ事業体に対する請求データとするとき各明細データを識別する識別データである。

【００３１】ＥＭ事業体は受け取った請求データの処理を検証処理と決済処理に分けて並行処理する。図５には検証処理のフローチャートを示す。ステップＳ５１で一括して処理する商品購入の明細データから一つずつ取り出す。ステップＳ５３において電子マネーが使われたときに明細データの電子署名Φ が作られたときに使用されたものと同じハッシュ関数を用いて改めて電子署名Φ を生成する。

【００３２】ステップＳ５４で明細データに添付されていた電子署名Φ と比較して、これが一致しないことを検出したときはこの明細データについて何らかの変更が加えられたとして決済処理を取り消さなければならない。すなわち、ステップＳ５５で取消処理を起動する。このとき、処理中のデータ識別番号を通知する。

【００３３】図６に決済処理のフローチャートを示す。後に説明する取消処理で設定するフラグについて説明しておく。並行して処理する検証処理で明細データに異常が検出されたとき取消処理が起動される分決済処理の進行状況によって通知された識別番号に対応する処理がまだ行われていないとき、すなわち検証処理の方が決済処理よりも先行しているときには、後ほど決済処理が行われるとき該当の識別番号の明細データは処理しないように取消フラグをＯＮとしておく。また、取消処理が起動されたとき該当の識別番号の決済処理中であればそのデータの処理終了時に直ちに戻し処理を行うように戻しフラグを設定して決済処理に通知する。

【００３４】決済処理は、まず、一括処理する明細データをステップＳ６１で一つずつ取り出す。ステップＳ６３で取消フラグがＯＮであるかを確認する。ＯＮのときは決済処理は行わないように次のデータの処理に戻る。

【００３５】ステップＳ６４では、明細データにある各種コードのチェックを行いどれだけの金額をどの口座間で決済すればよいのかを記憶する。ステップＳ６５において上記記憶した口座間で振替処理を行う。ステップＳ６５でこれらの処理を振替ログとして記録する。

【００３６】ステップＳ６７で、いま終わった一つの明細データについての処理が進行中に取消処理が起動され戻りフラグがＯＮとなっていないかを調べる。ＯＮのときはステップＳ６８で、処理した明細データについて戻し処理を行う。

【００３７】図７は取消処理のフローチャートである。取消処理は検証処理において明細データに異常が見つかったときに起動されるものである。どの明細データに異常が発生したかをデータ識別番号で通知されるのでステップＳ７１でこれを記憶する。起動されたときにその識別番号のデータの処理がまだ処理されていない状態ならステップＳ７２、ステップＳ７４で取消フラグをＯＮとする。また、そのデータの決済処理が進行中のときにはステップＳ７３、ステップＳ７５で戻しフラグをＯＮとする。

【００３８】起動されたとき識別番号で示されるデータが既に決済処理済であるときにはステップＳ７６でデータ識別番号に対応する振替ログにより戻し処理を実行する。これにより、このデータについての決済処理がなされなかったことになる。ここには示していないが、検証処理が検出した異常はデータ識別番号が記憶され別途原因の追求が行われる。

【００３９】

【発明の効果】以上の説明から明らかなように、本発明によれば、電子マネーの使用時の明細データの決済処理のように大量のデータを一括して処理する場合に、電子

署名など高度のデータセキュリティ強度を持たせると、データに改ざんがないことを検証するのに多くの時間を要するが、セキュリティを保証しながら且つ本来のデータの加工処理の時間を遅くすることがないようにしたデータ処理装置を提供でき、コンピュータシステムの運用時間の短縮と処理の信頼性向上、という著しい工業的効果がある。

【図面の簡単な説明】

【図１】　本発明の構成図

【図２】　本発明の実施の形態の説明図

【図３】　本発明の実施の形態の構成図

【図４】　商品購入データの形式の説明図

【図５】　検証処理のフローチャート

【図６】　決済処理のフローチャート

【図７】　取消処理のフローチャート

【図８】　従来技術の説明図

【符号の説明】

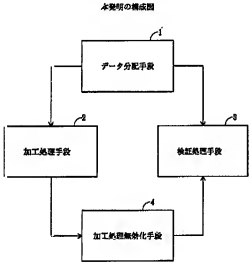
1　データ分配手段

2　加工処理手段

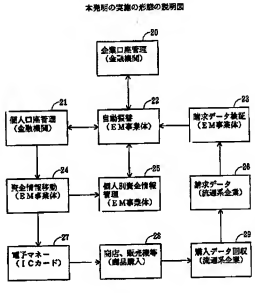
3　検証処理手段

4　加工処理無効化手段

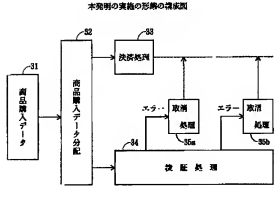
【図１】



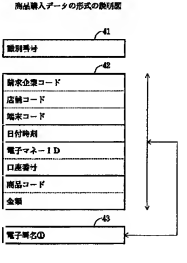
【図２】



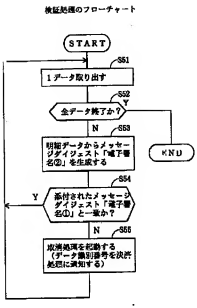
【図３】



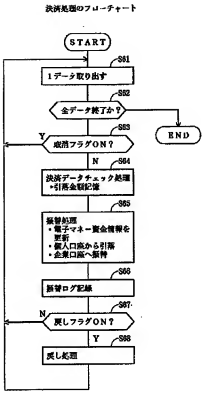
【図４】



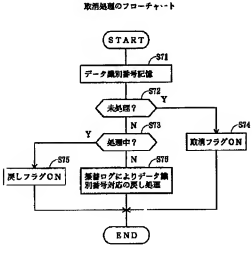
【図5】


検証処理のフローチャート
START
S51
1データ取り出す
S52
全データ終了か？
Y
N
S53
初期データからメッセージダイジェスト「端子番名①」を生成する
END
S54
添付されたメッセージダイジェスト「端子番名①」と一致か？
Y
N
S55
取消処理を起動する（データ識別番号を決済処理に通知する）

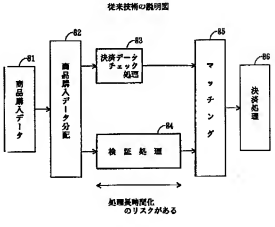
【図6】


決済処理のフローチャート
START
S61
1データ取り出す
S62
全データ終了か？
END
S63
取消フラグON？
Y
N
S64
決済データチェック処理
+引落金額記憶
S65
振替処理
・電子マネー資金情報を更新
・個人口座から引落
・企業口座へ振替
S66
振替ログ記録
S67
戻しフラグON？
N
Y
S68
戻し起動

【図7】


取消処理のフローチャート
START
S71
データ識別番号記憶
S72
未処理？
Y
N
S73
処理中？
Y
N
S74
取消フラグON
S75
戻しフラグON
S76
振替ログとよりデータ識別番号対応の戻し起動
END

【図8】


従来技術の説明図
81
商品購入データ
82
商品購入データ分配
83
決済データチェック処理
84
検証処理
85
マッチング
86
決済処理
処理長時間化のリスクがある